CLAIMS

1. Method for verifying a signature, or respectively an authentication, by means of an asymmetric private-key and public-key cryptographic calculation process between a "*prover*" entity and a "*verifier*" entity, the prover entity performing cryptographic calculations with said private key in order to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on this response value, performing cryptographic calculations with said public key in order to perform this signature verification, or respectively this authentication, the cryptographic calculation operations implementing the calculation of the modulo-n or large-number multiplications, characterized in that for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, it comprises the following steps"

- calculating at the level of said prover entity at least one prevalidation value;
- transmitting from the prover entity to the verifier entity at least said one prevalidation value, this prevalidation value allowing the verifier entity to perform at least one modular reduction without any division operation for this modular reduction.

2. Method according to claim 1, characterized in that for a public exponent e=2, the cryptographic calculation processing being based on a RABIN algorithm, said at least one prevalidation value comprises a unique value, which is the quotient Q of the square of said respective value of a signature or a response by said public modulo n, Q = R*R/n, where R designates said respective value of a signature or a response to an authentication.

3. Method according to claim 2, characterized in that after the reception by said entity of said respective value of a response to an authentication verification or a signature of a message (M), and of said at least one prevalidation value comprising said quotient, this method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{AR}, D_{SR}) between the square of the response value R*R and the product Q*n of said quotient Q by said public modulo n, (D_{AR}, D_{SR} = R*R – Q*n;

- verifying the equality of said difference with the value of a function of this response value, without any division operation by the modulo n operation.

4. Method according to claim 1, characterized in that for a public exponent e = 3, the cryptographic calculation process being based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient Q_1 of the square R*R of said response value R by said public modulo n;

- a second quotient Q_2 of the product of said response value and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, by said public modulo n, Q_2 = R*(R*R – Q_1*n)/n.

5. Method according to claim 4, characterized in that after the reception of said response value R and said at least one prevalidation value comprising said first and second quotients Q_1 and Q_2, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{ARSA}, D_{SRSA}) between the product of said response value R and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, and the product of said second quotient Q_2 and said public modulo n (D_{ARSA}, D_{SRSA}) = R*(R*R – Q_1*n)-Q_2*n;

- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo n operation.

6. Method according to claim 3 or 5, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of this message M, it comprises the following steps:

- applying a condensation function to this message in order to obtain a message digest CM;

- concatenating this message digest with a constant value.

7. Method according to either claim 3 or 5, characterized in that, for an authentication verification operation, this method also comprises the step for transmitting an prompt value from the verifier entity to the prover entity.

8. Method according to claim 7, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

9. Method according to either of claims 3 and 7, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

10. Method according to claim 9, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises the calculation of the value C*A and the storing of this value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that the calculation of said function f(A) = -C*A modulo n comprises the calculation of the value n-C*A and the storing of this value if n-C*A ≥ 0, and otherwise the calculation of the intermediate value C*n-C*A, and if this intermediate value is greater than or equal to zero, the calculation and storing of the value of -C*A modulo n, which makes it possible to verify the equality of said authentication without any division for the modular reduction.

11. Method according to claims 5 and 8, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify